ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

IMPLEMENTACIÓN DE UN SISTEMA DE TRANSMISIÓN Y RECEPCIÓN DE TEXTO CIFRADO EN UN MEDIO INALÁMBRICO USANDO MODULACIONES QPSK Y PI/4 QPSK CON OFDM

EXAMEN COMPLEXIVO, COMPONENTE PRÁCTICO
INFORME DE PROYECTO

Previa a la obtención del Título de:

MAGISTER EN TELECOMUNICACIONES

Presentado por:

Ing. Othón Andrés Ponce Alvarado

GUAYAQUIL - ECUADOR

AÑO 2016

AGRADECIMIENTOS

Agradezco de manera especial y sincera a mi coordinador de la maestría al Ph.D. Boris Ramos, por su apoyo y su capacidad para guiar mis ideas, ha sido un aporte invaluable en el desarrollo de este trabajo.

DEDICATORIA

Dedico este logro alcanzado de forma especial a Dios, a mi esposa Gabriela Montesdeoca, a mi madre Sara Alvarado Loor y a mis hermanos Sara e Isaías Ponce Alvarado, gracias por siempre estar conmigo y ser los pilares fundamentales de mi vida.

TRIBUNAL DE SUSTENTACIÓN

M. Sc. Washington Medina

EVALUADOR

M.Sc. Nestor Arreaga.

EVALUADOR

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este Informe de Proyecto, me corresponde exclusivamente; y el patrimonio intelectual del mismo, a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL".

Art. 12 del Reglamento de Graduación.

Othón Ponce Alvarado

Othón Andrés Ponce Alvarado

C.I.: 0919347757

RESUMEN

En el presente documento se detalla el desarrollo, análisis e implementación de un sistema de comunicación inalámbrica por medio de equipos de radio frecuencia definido por software usando los NI Universal Software Peripheral Radio (USRP) y el software LabVIEW. El sistema está compuesto por transmisor, receptor y canal con ruido. El proyecto consiste en enviar texto como fuente de datos usando OFDM, dicho texto es modulado mediante QPSK o π/4 QPSK y transmitido mediante los equipos de radio USRP 2920. Cabe mencionar que el texto antes de ser enviado es sometido a un procesamiento de datos el cual se encarga de cifrar la información y luego se aplica codificación convolucional en el lado del transmisor, el proceso inverso se realiza en el receptor. Las mediciones tomadas fueron de Bit Error Rate (BER) y Signal to Noise Ratio (SNR) obtenidos en diferentes contextos como un ambiente simulado y real. Para el ambiente simulado se utilizó la herramienta de desarrollo de sistemas Labview y en el ambiente real se usó los USRP. Finalmente, se realizaron comparaciones del SNR, BER y la tasa de bits de los diferentes canales de cada modulación.

CONTENIDO

ABREVIATURAS

BER	Bit Error Rate
D	Ecualizador Directo
ISI	Interferencia Intersimbólica
MMSE	Error Cuadrático Promedio Mínimo
MSE	Error Cuadrático Promedio
OA	Outdoor A
OB	Outdoor B
QPSK	Quadrature Phase-Shift Keying
S	Simulado
SNR	Signal to Noise Ratio
USRP	Universal Software Radio Peripheral

LISTA DE FIGURAS

LISTA DE TABLAS

INTRODUCCIÓN

En la actualidad existen diferentes formas de transmisión de comunicación, una de ellas es la comunicación inalámbrica y como en cualquier tipo de comunicación se requiere garantizar que los datos se transmitan de manera rápida, segura y eficiente; para evitar pérdida de datos durante la transmisión y asegurar que los datos trasmitidos no puedan ser recibidos por terceros y en el caso de que los mensajes transmitidos sean interceptados por terceros, estos no puedan interpretar el contenido del mensaje por medio de la técnica de cifrado.

Para garantizar la transmisión del mensaje de forma eficiente, es necesario usar un método como el Orthogonal Frequency Division Multiplexing (OFDM) [1].

OFDM es un esquema de ancho de banda multiportadora eficiente para comunicaciones digitales en la que se evidencia que subportadoras se superponen a otras, logrando que el espectro sea más eficiente.

El objetivo de este documento es mostrar el diseño e implementación de un sistema de comunicación inalámbrico usando los NI USRP modelo 2920, que tienen un rango de frecuencias desde 50 MHz hasta 2.2GHz, lo cual permite cubrir radios FM, GPS, GSM y usando software LabVIEW para generar este proyecto.

1. MARCO TEORICO

En este capítulo se realizará una breve introducción sobre las modulaciones implementadas, los diferentes canales multipaso que fueron emulados, el tipo de información que fue transmitido, el cifrado, entre otras.

1.1. OFDM

Orthogonal Frequency Division Multiplexing (OFDM) es una tecnología de comunicación inalámbrica que es muy popular hoy en día. OFDM ha sido adoptado en estándares inalámbricos, tales como la radiodifusión de audio digital (DAB), Digital Video Broadcasting (DVB-T), estándar para redes de área local (LAN) IEEE802.11 [2].

OFDM es un multiportadora eficiente de ancho de banda de la comunicación digital donde la frecuencia de la subportadora de OFDM se superpone al otro de modo que el espectro es eficiente [3].

OFDM es una tecnología inalámbrica que utiliza la técnica de dividir la señal portadora en varias señales subportadoras que son ortogonales entre sí. Múltiple señales de subportadora ortogonales se superponen en el espectro,

los cuales puede ser generado por la generalización el criterio de portadora simple de Nyquist en un criterio de múltiples portadoras.

En la práctica, la superposición de frecuencias de OFDM puede ahorrar el uso de la frecuencia. En el esquema OFDM, hay un intervalo de guarda en el dominio del tiempo que se llama prefijo cíclico (CP). Este CP puede reducir la interferencia inter-simbólica (ISI) [4].

La modulación puede ser BPSK, QPSK, π/4 QPSK, QAM u otro. Entonces a la señal modulada se aplica la Transformada Inversa Discreta de Fourier (IDTF), para generar símbolos OFDM. Esto permite el uso de la frecuencia y realizar asignaciones ortogonales entre sí.

Este trabajo hace uso de los equipos USRP, los cuales tienen como procesador tarjetas FPGA, puerto Gigabit Ethernet, antena, cable MIMO, adaptador de corriente, tal como se muestra en la Figura 2.

Fig. 1. NI USRP-2920. [4]

1.2. QPSK

Quadrature phase-shift keying (QPSK) aumenta la capacidad y las longitudes de la señal de transmisión. Procesamiento de banda base, en la tasa de símbolos permite mantener el bajo ancho de banda requerido electrónica.

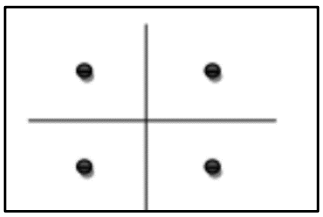


Fig. 2. Constelación de QPSK

1.3. CRIPTOGRAFÍA

Se define a la criptografía como la disciplina que se encarga del estudio de códigos secretos o también conocidos como códigos cifrados [5].

Igual que otro autor define a la criptografía como la técnica de convertir un texto claro conocido como texto plano, en otro, llamado criptograma

ciphertex, donde el contenido de la información es igual al anterior, pero sólo lo pueden entender las personas autorizadas [6].

De la misma manera, otro autor señala que la criptografía es la técnica que se utiliza para cifrar mensajes ya que proviene del griego Kryptos que significa “escondido” y Graphein que significa “escritura” [7].

Si bien es cierto existen varias definiciones sobre criptografía los autores coinciden en que es una ciencia de la escritura secreta que tiene como objetivo ocultar el significado de un mensaje [8].

1.3.1. CRIPTOGRAFÍA SIMÉTRICA

La criptografía simétrica o cifrada de clave privada, consiste en utilizar una sola clave para cifrar como para descifrar los datos. La clave debe distribuirse antes de la transmisión entre las entidades que van a recibir el mensaje. La robustez del cifrado de clave simétrica depende del tamaño de la clave privada utilizada. Los algoritmos criptográficos simétricos incluyen más comunes son DES, 3DES, Blowfish y AES [9].

Para otros autores el principio de cifrado de clave simétrica se basa en dos propiedades: la primera es que la clave secreta para el cifrado es la misma para el descifrado, la segunda es que el cifrado y la función de descifrado son bastante similares.

Los algoritmos simétricos tales como AES o 3DES son muy seguros, rápidos y de uso generalizado.

Cuando se usan esquemas con clave simétrica hay varios inconvenientes asociados ya que el problema es la distribución de la clave, dado que el enlace de comunicación para el mensaje no es seguro, el envío de la clave a través de este canal no es posible, en vista de que el emisor y el receptor poseen la misma clave, por lo que la criptografía simétrica no se puede utilizar para aplicaciones donde se necesita comprobar la identidad del emisor o receptor [8].

1.3.2. CRIPTOGRAFÍA ASIMÉTRICA

El cifrado de clave asimétrico o cifrado de clave pública se utiliza para resolver el problema de distribución de claves que tiene la criptografía simétrica.

En las claves asimétricas, dos claves son usadas; y se clasifican en claves privadas, las cuales se utilizan para el descifrado y las claves públicas que se utilizan para el cifrado.

Dado que los usuarios utilizan dos claves: la clave pública, que es conocida y la privada que se mantiene en secreto. Con base a lo anteriormente mencionado, de esta manera no hay necesidad de realizar la distribución de las claves antes de la transmisión.

Las técnicas de cifrado asimétricos son casi 1.000 veces más lentos que las técnicas simétricas, ya que requieren más potencia de procesamiento computacional [9].

Con el fin de superar los inconvenientes en el cifrado de simétrico Diffie, Hellman y Merkle tenían una revolucionaria propuesta basada en la siguiente idea: no es necesario que la clave que posee la persona que cifra el mensaje sea secreto, la parte crucial es que el receptor, sea el único que pueda descifrar utilizando una clave secreta, de tal manera que el receptor tiene una clave pública que es conocida por todos y también tiene una clave secreta que utiliza para el descifrado [8].

1.4. CIFRADO

En este proyecto el texto transmitido se cifra a nivel de bits, en el cual el texto plano se convierte a bits, y luego los bits se invierten y estos a su vez se combinan con los bits del texto original, de esta manera cifra el texto a transmitir y se concluye en que se vuelven a colocar los datos en un arreglo de una sola dimensión.

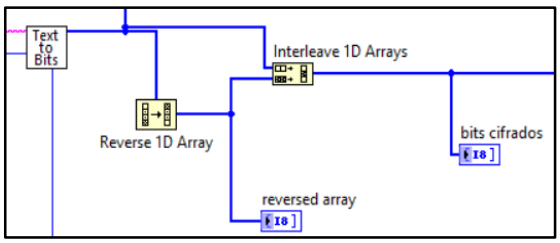


Fig. 3. Bloque de cifrado.

1.5. CANALES DE COMUNICACIÓN

Un canal de comunicación es un medio de transmisión por el que se transmiten las señales portadoras de información entre el emisor y receptor.

Los canales de comunicación usados en el proyecto son multi-paso, lo que genera que la señal llega con diversos retardos y se atenúe. Conjuntamente cuando se incrementa la potencia de la señal, también aumenta la potencia

del ISI, por lo cual se representa en los escenarios Outdoor como se pueden observar en la Tabla 1.

Tabla 1. Canales Outdoor - Áreas Rurales.

Item	Canal A		Canal B	
	Delay (uSec)	Avg. Power (dB)	Delay (uSec)	Avg. Power (dB)
1	**0.0**	**0.0**	**0.0**	**0.0**
2	**0.2**	**-2.0**	**0.1**	**-4.0**
3	**0.4**	**-10.0**	**0.2**	**-8.0**
4	**0.6**	**-20.0**	**0.3**	**-12.0**
5			**0.4**	**-16.0**
6			**0.5**	**-20.0**

2. IMPLEMENTACIÓN

Para la implementación del sistema de transmisión y recepción inalámbrico usando modulaciones QPSK y PI/4 QPSK se usaron como base las prácticas realizadas en el laboratorio adoptándolas para las modulaciones de este proyecto. [19]

La figura 3 y 4 muestra el bloque transmisor y receptor; y el hardware utilizado, respectivamente.

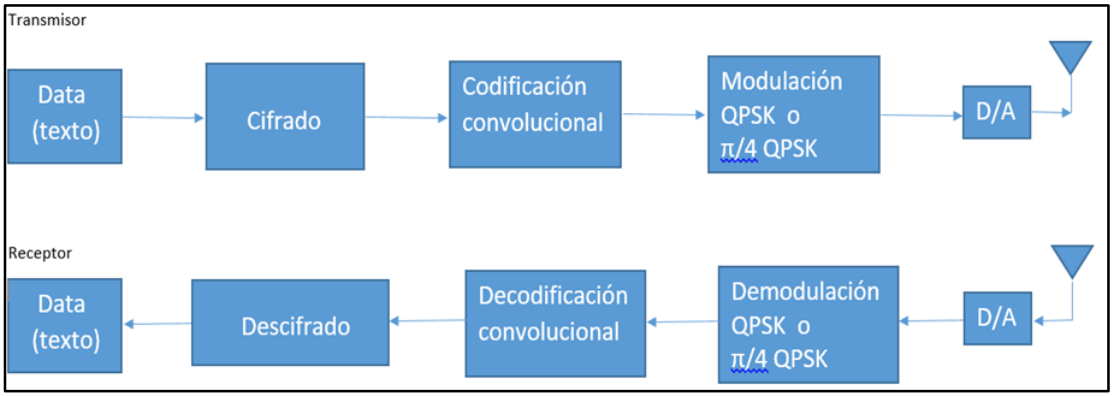


Fig. 4. Bloque transmisor y receptor.

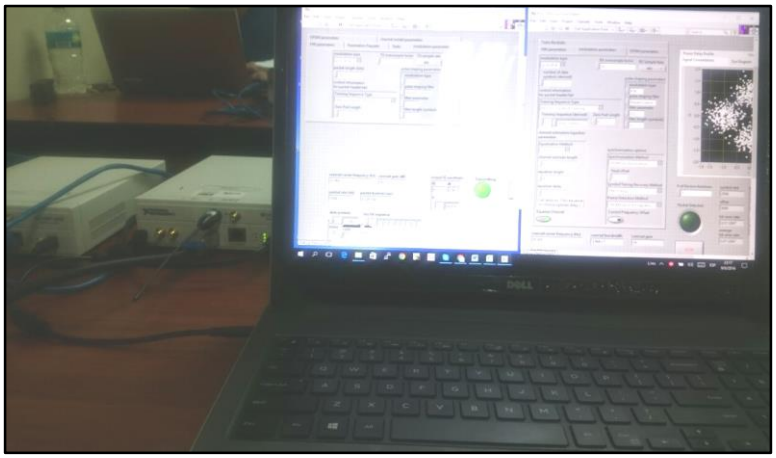


Fig. 5. Hardware utilizado.

Además, se tomaron en consideración algunos parámetros, los cuales se muestran en la Tabla 2.

Tabla 2. Parámetros del proyecto.

Proyecto 23	EXPANSIÓN DE OFDM
Tipo de Información	Texto
Modulación	QPSK – π/4 QPSK
Canal	Real – Tabla 1
Codificación del Canal 2	Convolucional
Cifrad0o	Definida por el Ingeniero

El tipo de dato que fue usado como fuente de transmisión fue texto plano tal como se puede observar en la figura 6.

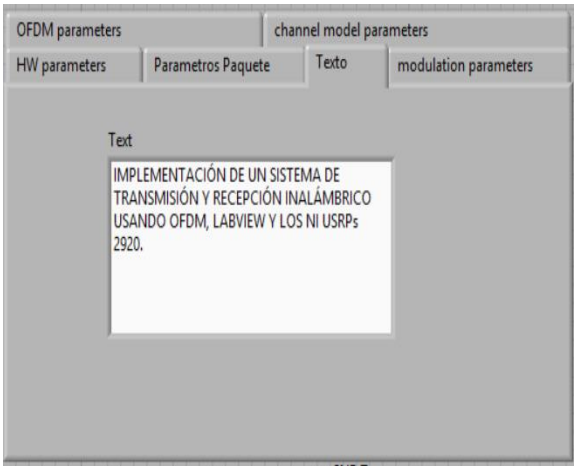


Fig. 6. Texto plano a transmitir.

Una vez ingresado el texto, la programación implementada con la herramienta LabVIEW permite enviar el texto al siguiente bloque, el cual se encarga de cifrar el mensaje de texto utilizando el algoritmo de cifrado escogido, que para nuestro caso de estudio se cifra el mensaje invirtiendo el orden de los bits y se combina con los bits originales, tal como se muestra en la figura 7.

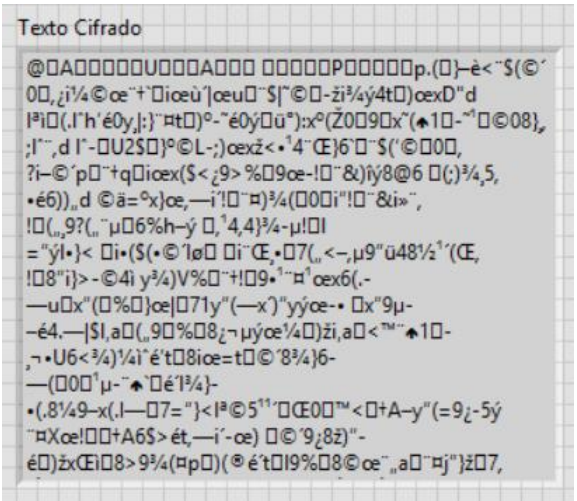


Fig. 7. Texto cifrado.

Una vez que se ha cifrado el texto, los bits pasan por el codificador convolucional, tal como se muestra en la Figura 8.

Fig. 8. Muestra de los bits convolucionados.

El siguiente paso será aplicar la modulación QPSK o π/4 QPSK según sea el caso, en las figuras 9, 10, 11 y 12 se muestran las constelaciones del transmisor y receptor.

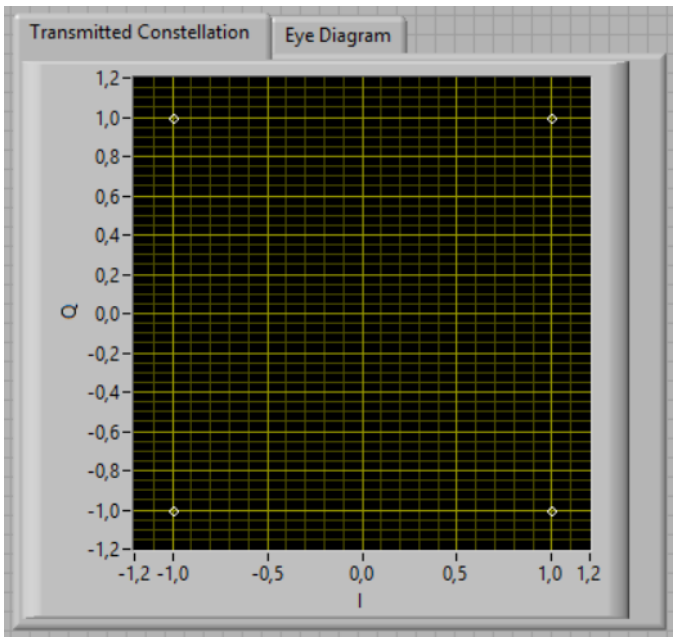


Fig. 9. Constelación QPSK en el transmisor.

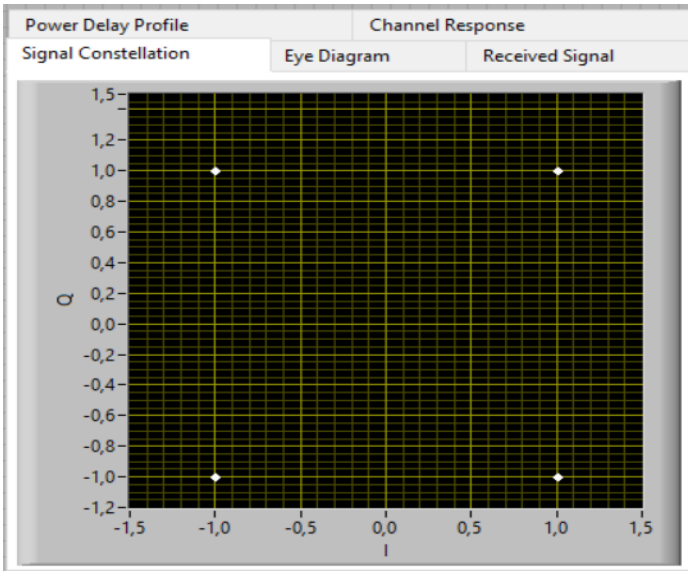


Fig. 10. Constelación QPSK en el receptor.

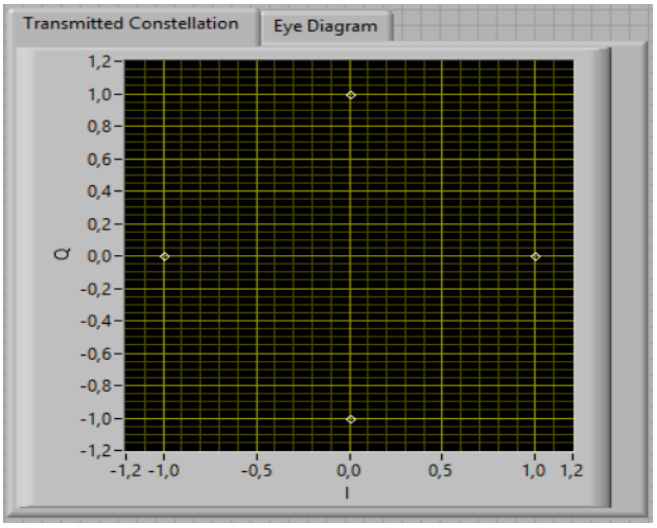


Fig. 11. Constelación π/4 QPSK en el transmisor.

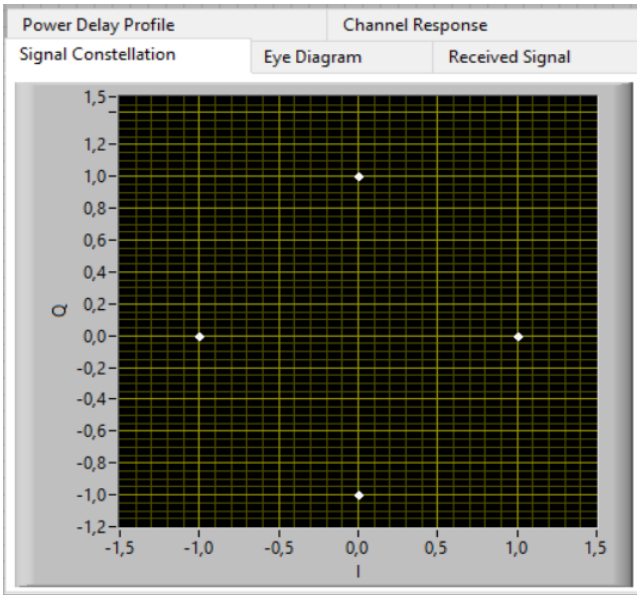


Fig. 12. Constelación π/4 QPSK en el receptor.

En el receptor se realiza el proceso inverso a cada bloque implementado, y al final se muestra el texto recibido como se observa en la figura 13.

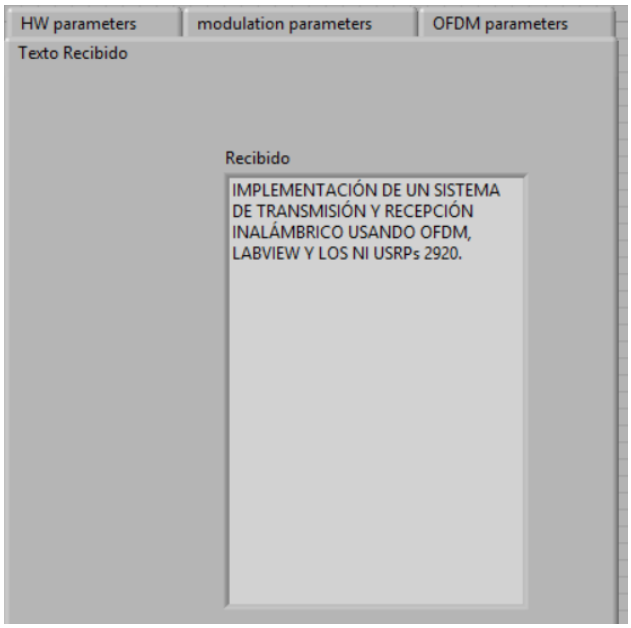


Fig. 13. Texto recibido.

3. ANÁLISIS Y RESULTADOS

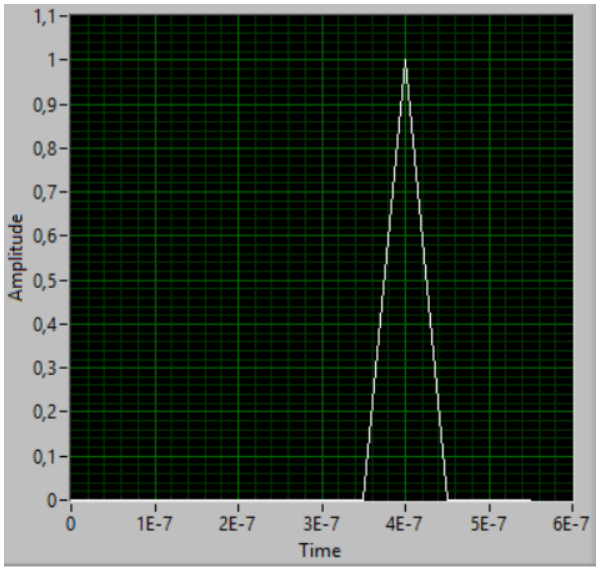
Las pruebas fueron desarrolladas en el campus de la Escuela Superior Politécnica del Litoral (ESPOL).

Se realizó la toma de datos simulados mediante la herramienta LabVIEW y la toma de datos reales con la ayuda adicional de los USRP.

Se analizaron tres tipos de gráficas las cuales son:

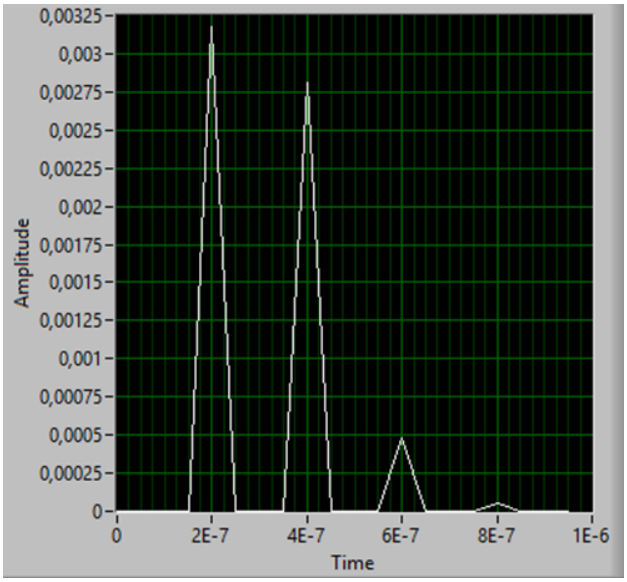
- Perfiles de retardo de Potencia.
- BER vs SNR.
- Rb vs SNR.

En las gráficas 1a, 1b y 1c se podrá observar la respuesta de los perfiles de retardo de potencia de un canal Real AWGN, canal multipaso con los valores de la Tabla 1, canal A y canal B respectivamente, usando modulación QPSK.



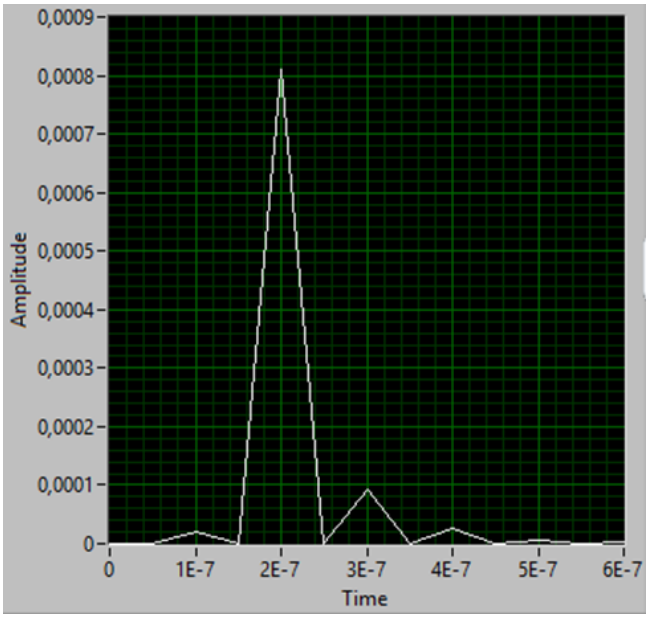
Gráfica. 14. Canal Real AWGN.

En la gráfica 1a se muestra 1 paso ubicado a 0.4 useg.



Gráfica. 15. Canal multipaso Tabla 1, canal A.

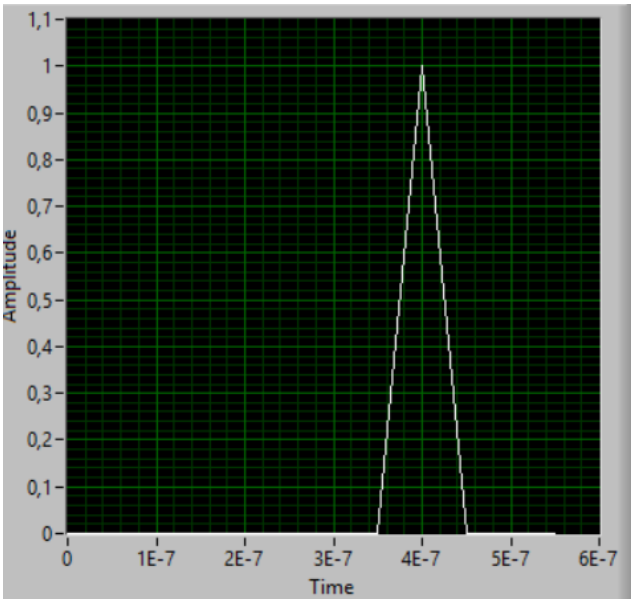
En la gráfica 1b se muestran 4 pasos ubicados a 0.2 useg.



Gráfica. 16. Canal multipaso Tabla 1, canal B.

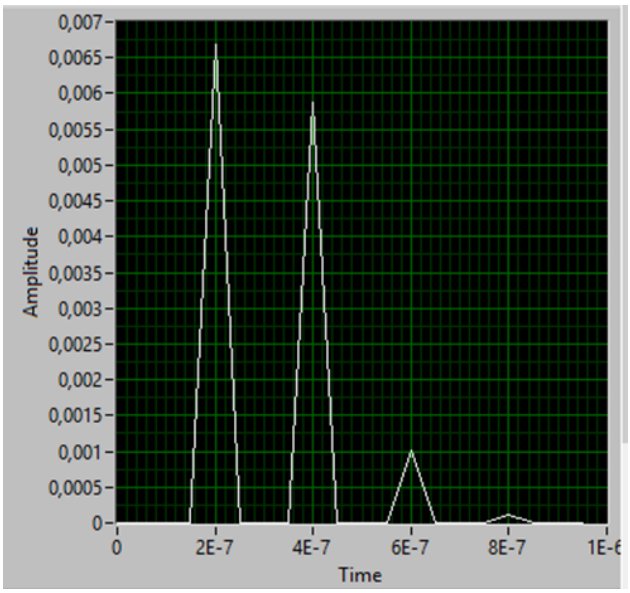
En la gráfica 1c se muestran 6 pasos ubicados a 0.1 useg.

En las gráficas 2a, 2b y 2c se observan las diferentes respuestas de los perfiles de retardo de potencia de un canal real AWGN y canales multipaso mostrados en la Tabla 1 Canal A y Canal B respectivamente usando modulación pi/4 QPSK.



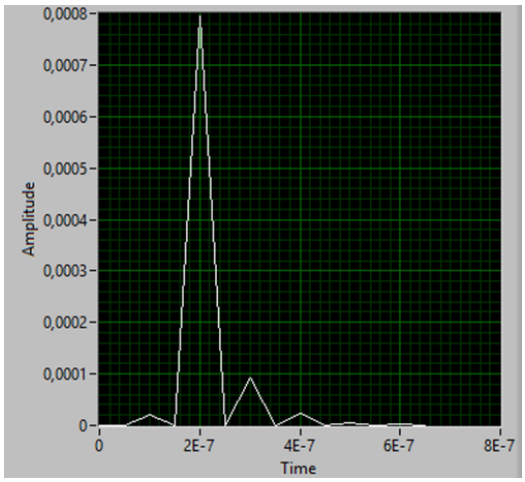
Gráfica. 17. Canal Real AWGN.

En la gráfica 2a se muestra 1 paso ubicado a 0.4 useg.



Gráfica. 18. Canal multipaso Tabla 1, canal A.

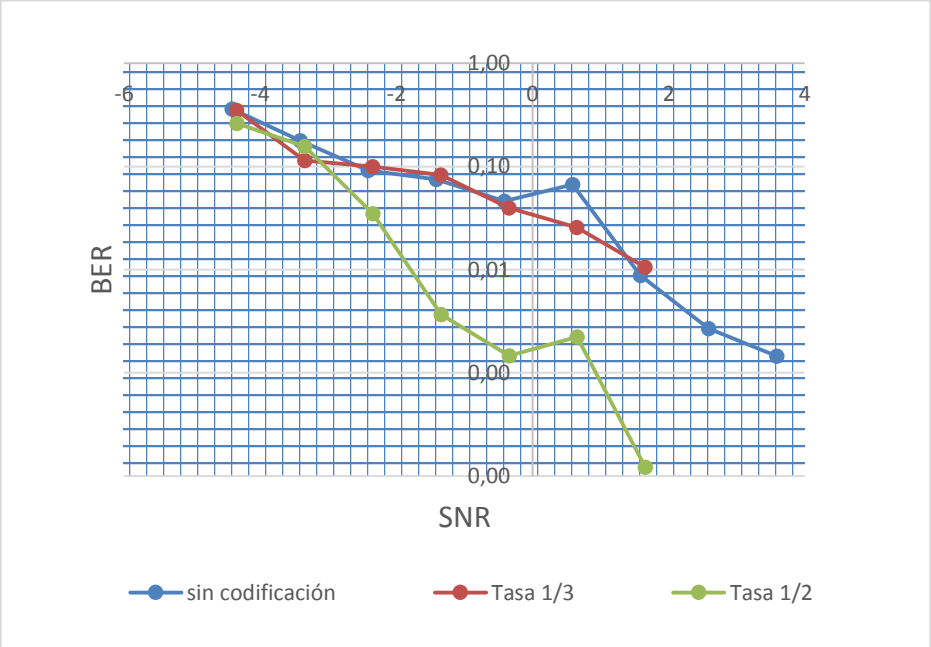
En la gráfica 2b se muestran 4 pasos ubicados a 0.2 useg.



Gráfica. 19. Canal multipaso Tabla 1, canal B.

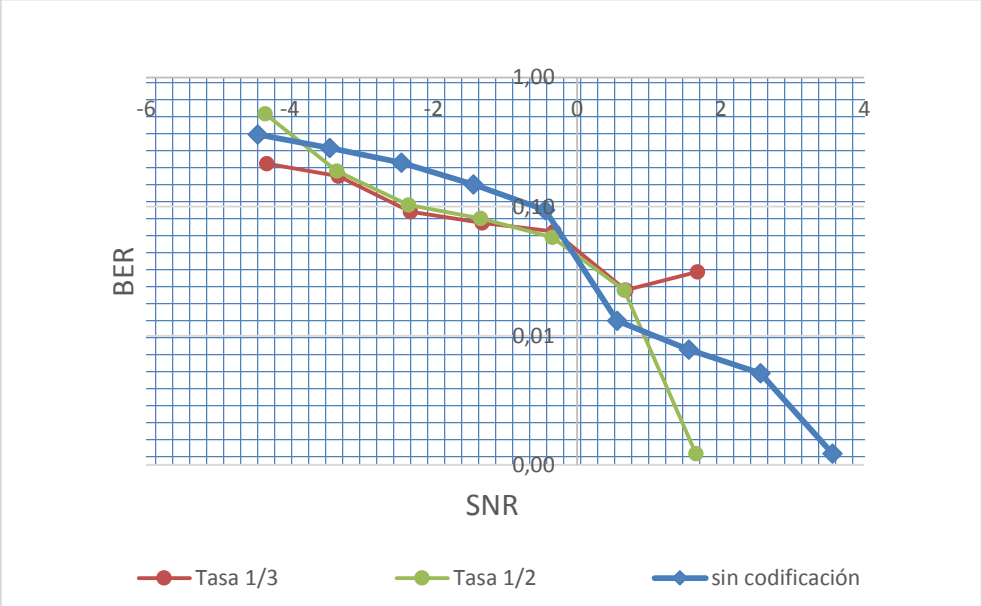
En la gráfica 2c se muestran 6 pasos ubicados a 0.1 useg.

En las siguientes gráficas se observan los valores de BER en relación al SNR, datos que fueron tomados usando los equipos USRP.



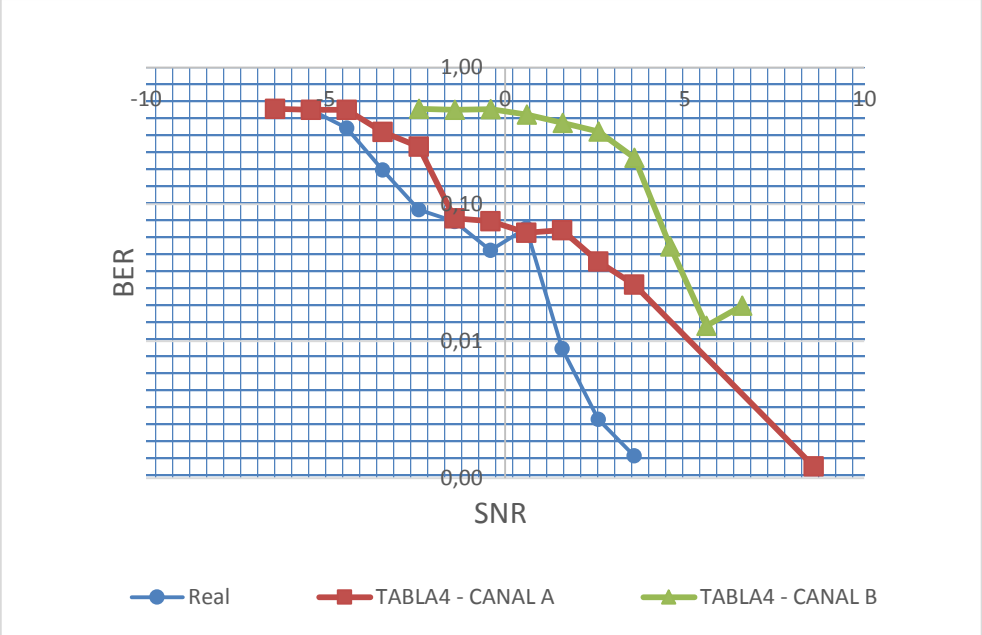
Gráfica. 20. BER vs SNR QPSK – Canal Real.

En la gráfica 3 se observa un análisis comparativo de modulación QPSK en un canal Real sin codificación de canal y con codificación convolucional con Tasa 1/2 y 1/3.



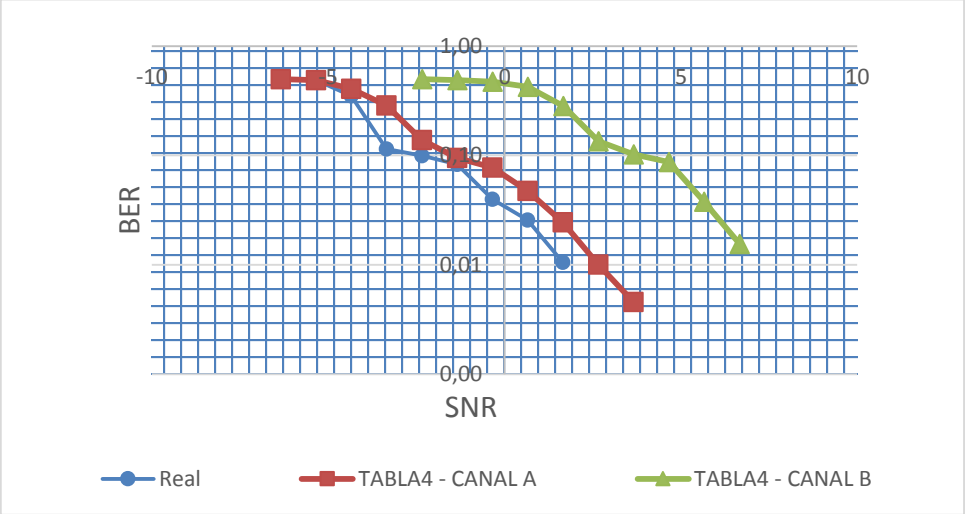
Gráfica. 21. BER vs SNR PI/4 QPSK – Canal Real.

En la gráfica 4 se observa un análisis comparativo de modulación PI/4 QPSK en un canal Real sin codificación de canal y con codificación convolucional con Tasa 1/2 y 1/3.



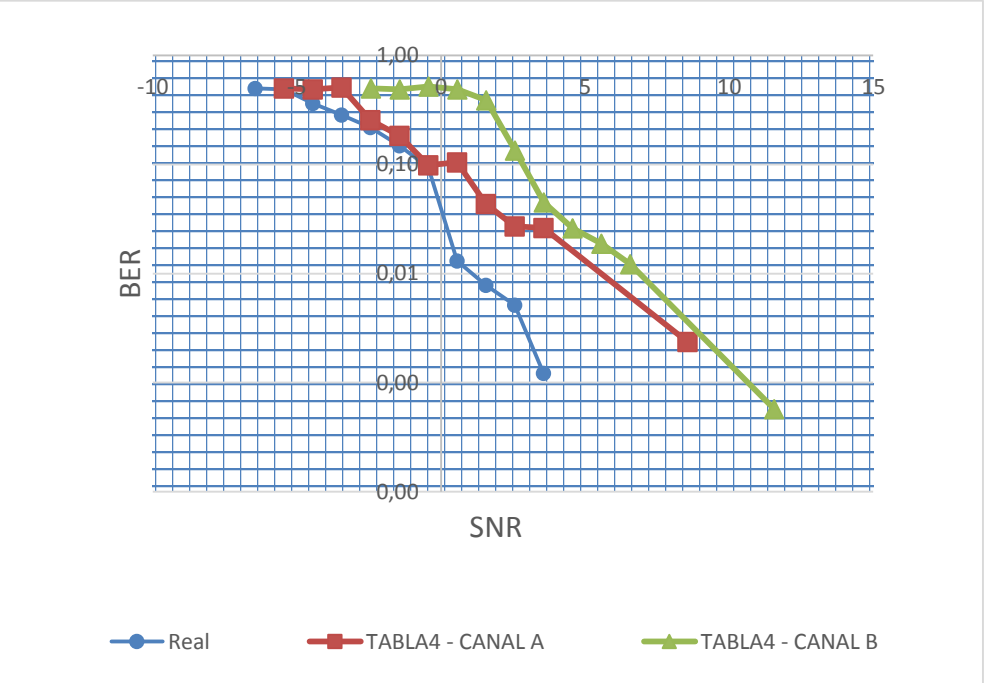
Gráfica. 22. BER vs SNR QPSK sin codificacion – canales varios.

En la gráfica 5 se observa un análisis comparativo de modulación QPSK sin codificación en canales varios (real, Tabla 1 canal A y canal B).



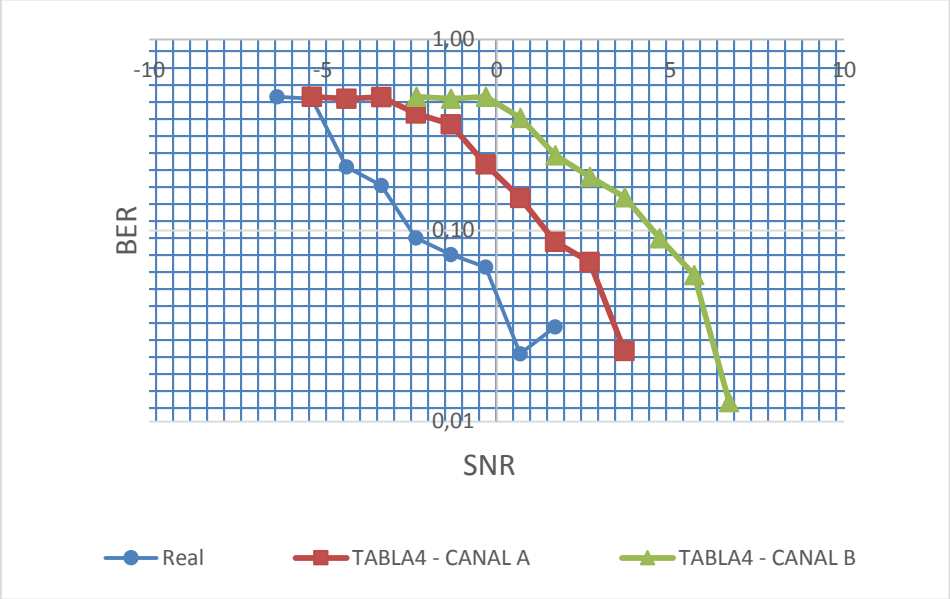
Gráfica. 23. BER vs SNR QPSK con codificacion tasa 1/2 – canales varios.

En la gráfica 6 se observa un análisis comparativo de modulación QPSK con codificación convolucional a una tasa de 1/2 en canales varios (real, Tabla 1 canal A y canal B).



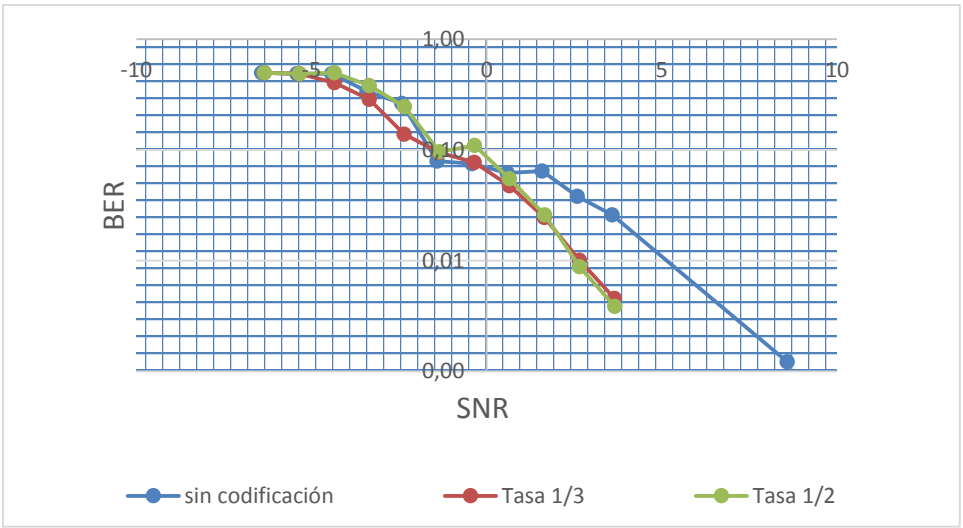
Gráfica. 24. BER vs SNR PI/4 QPSK sin codificacion – canales varios.

En la gráfica 7 se observa un análisis comparativo de modulación PI/4 QPSK sin codificación en canales varios (real, Tabla 1 canal A y canal B).



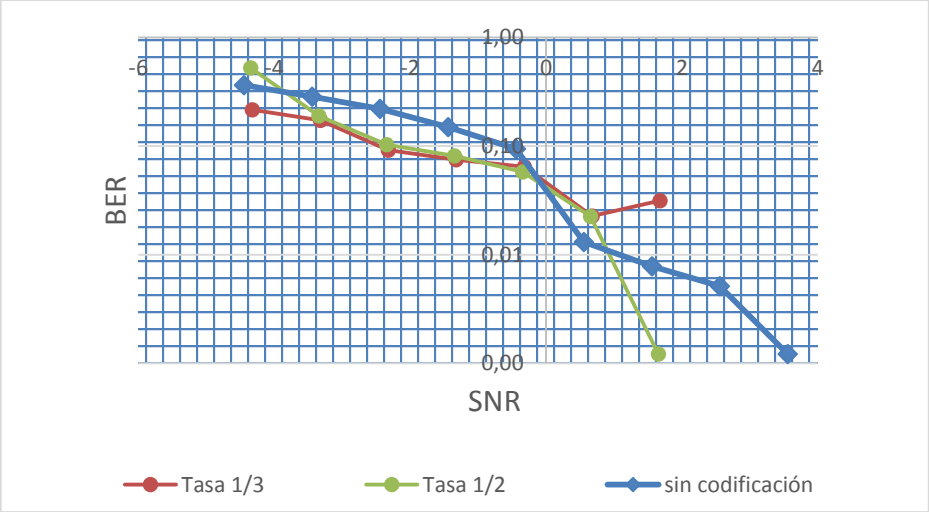
Gráfica. 25. BER vs SNR PI/4 QPSK con codificacion tasa 1/2 – canales varios.

En la gráfica 8 se observa un análisis comparativo de modulación PI/4 QPSK con codificación convolucional a una tasa de 1/2 en canales varios (real, Tabla 1 canal A y canal B).



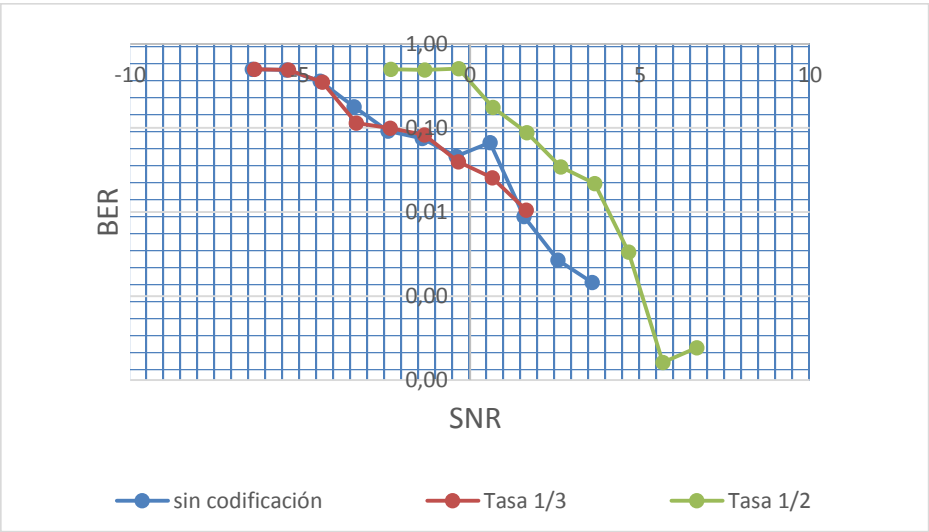
Gráfica. 26. BER vs SNR QPSK – Tabla 1 Canal A.

En la gráfica 9 se observa un análisis comparativo modulación QPSK con los datos de la Tabla 1 - canal A sin codificación de canal y con codificación convolucional Tasa a 1/2 y 1/3.



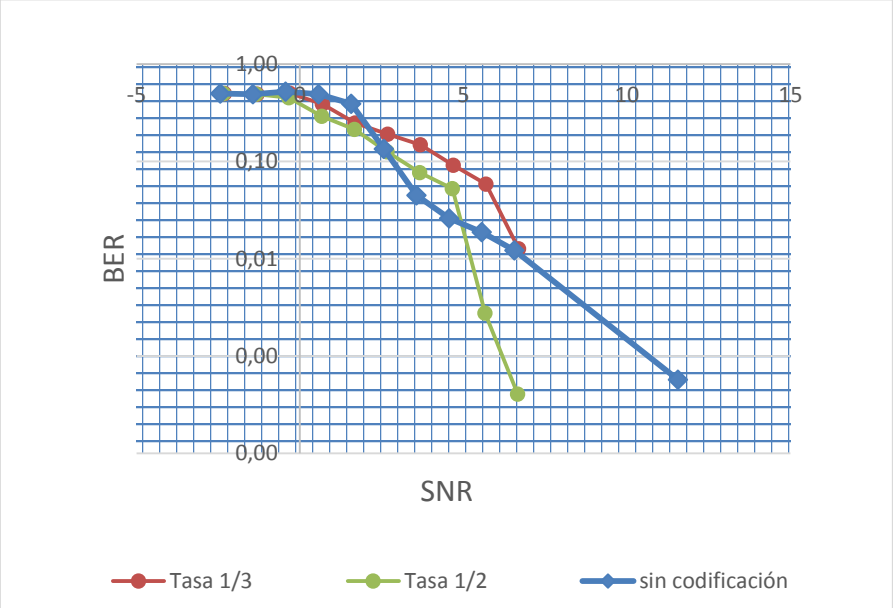
Gráfica. 27. BER vs SNR PI/4 QPSK – Tabla 1 Canal A**.**

En la gráfica 10 se observa un análisis comparativo modulación PI/4 QPSK con los datos de la Tabla 1 - canal A sin codificación de canal y con codificación convolucional Tasa a 1/2 y 1/3.



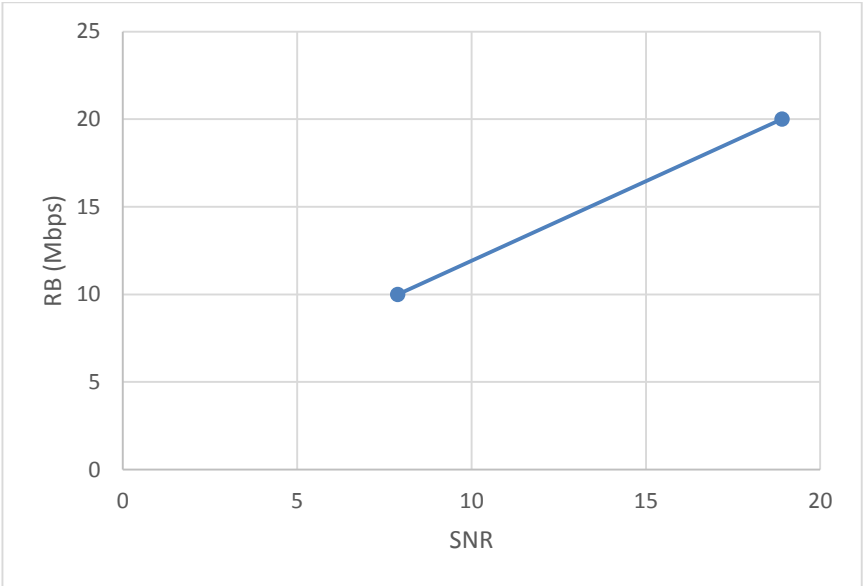
Gráfica. 28. BER vs SNR QPSK – Tabla 1 Canal B.

En la gráfica 11 se observa un análisis comparativo modulación QPSK con los datos de la Tabla 1 - canal B sin codificación de canal y con codificación convolucional Tasa a 1/2 y 1/3.



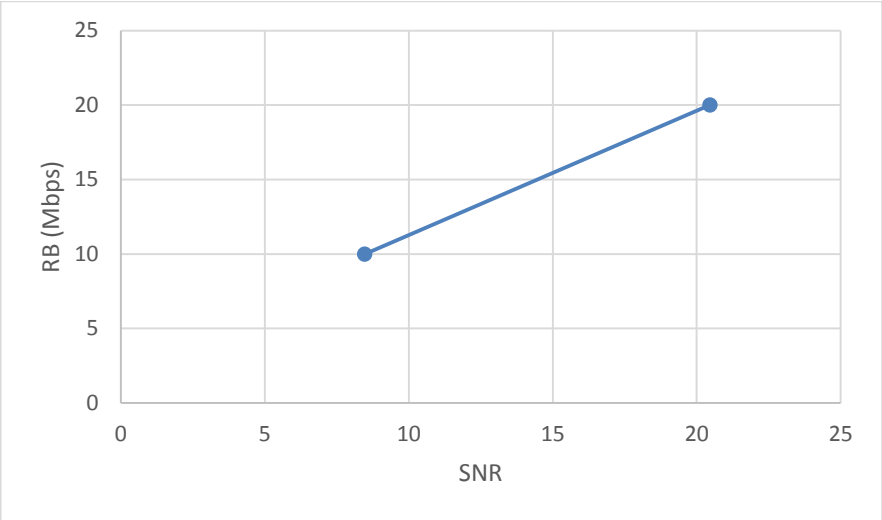
Gráfica. 29. BER vs SNR PI/4 QPSK – Tabla 1 Canal B.

En la gráfica 12 se observa un análisis comparativo modulación PI/4 QPSK con los datos de la Tabla 1 - canal B sin codificación de canal y con codificación convolucional Tasa a 1/2 y 1/3.



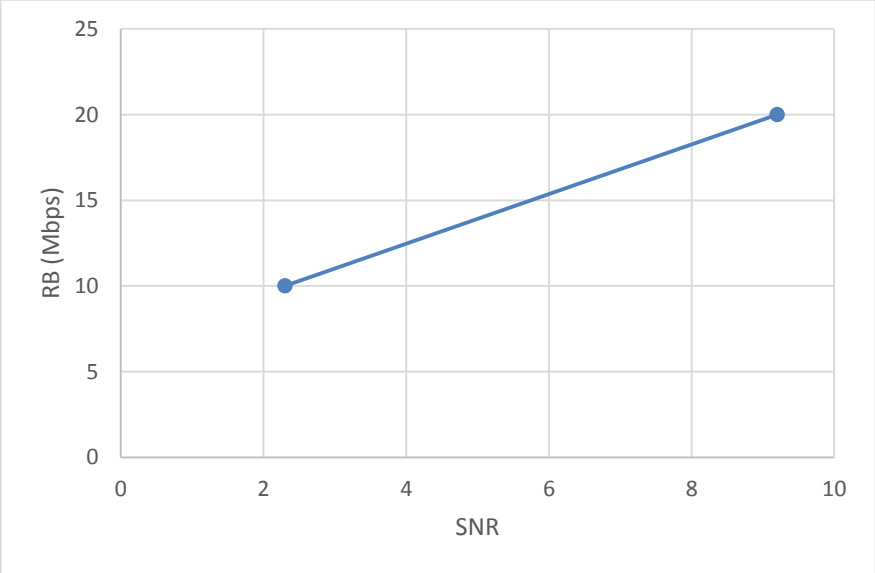
Gráfica. 30. Rb vs SNR QPSK – canal AWGN.

En la gráfica 13 se observa una tasa de transmisión máxima de 20Mbps con un SNR aproximado de 20dB con modulación QPSK sin codificación.



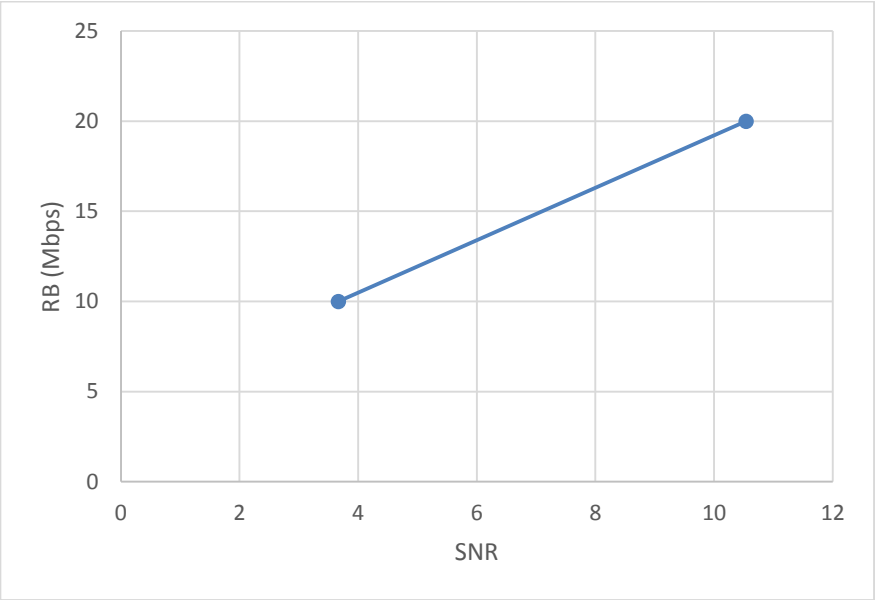
Gráfica. 31. Rb vs SNR QPSK – canal AWGN.

En la gráfica 14 se observa una tasa de transmisión máxima de 20Mbps con un SNR aproximado de 22dB con modulación QPSK con codificación convolucional 1/3.



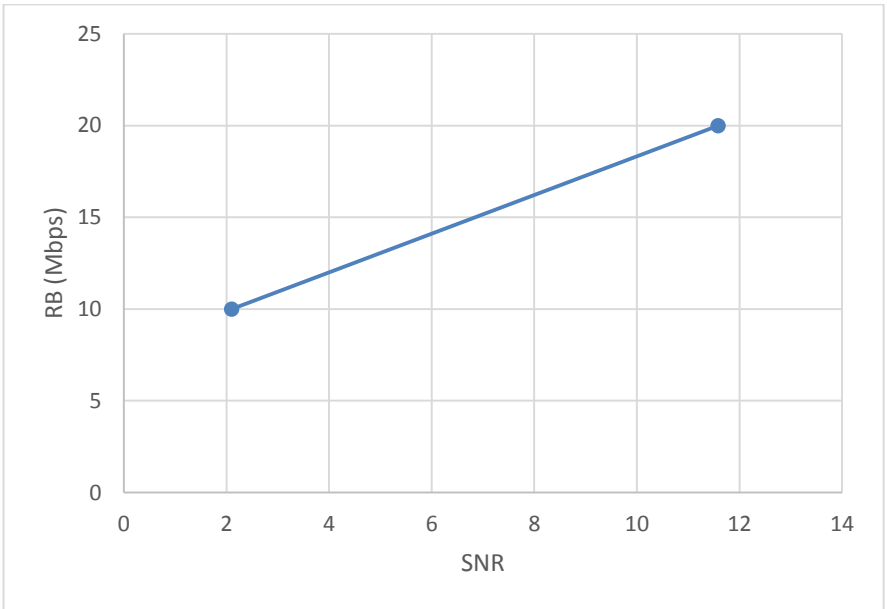
Gráfica. 32. Rb vs SNR QPSK – canal A Tabla 1.

En la gráfica 15 se observa una tasa de transmisión máxima de 20Mbps con un SNR aproximado de 9dB con modulación QPSK sin codificación.



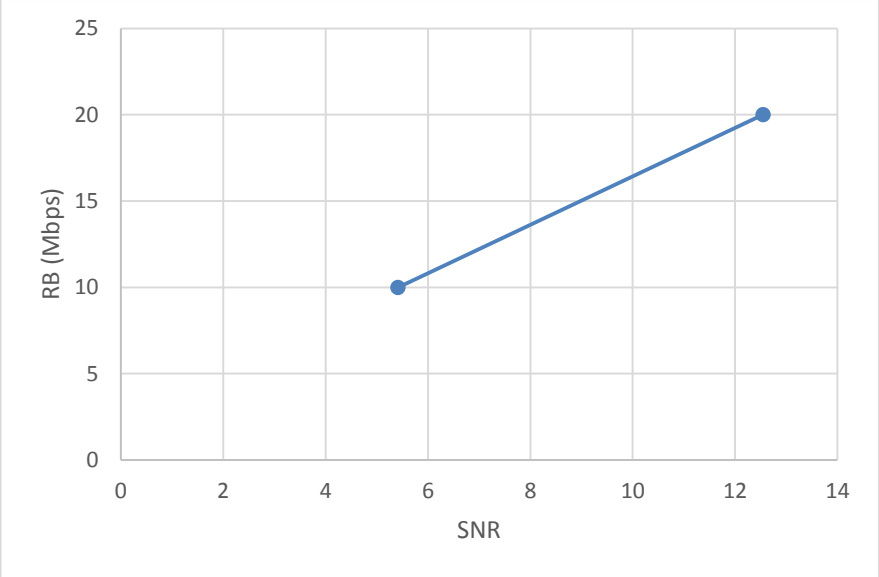
Gráfica. 33. Rb vs SNR QPSK – canal A Tabla 1.

En la gráfica 16 se observa una tasa de transmisión máxima de 20Mbps con un SNR aproximado de 11dB con modulación QPSK con codificación convolucional 1/3.



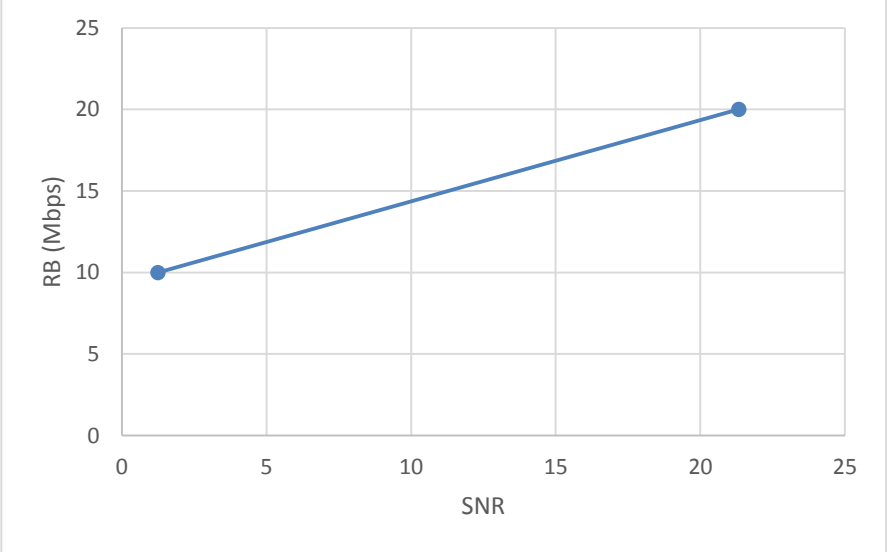
Gráfica. 34. Rb vs SNR QPSK – canal B Tabla 1.

En la gráfica 17 se observa una tasa de transmisión máxima de 20Mbps con un SNR aproximado de 12dB con modulación QPSK sin codificación.



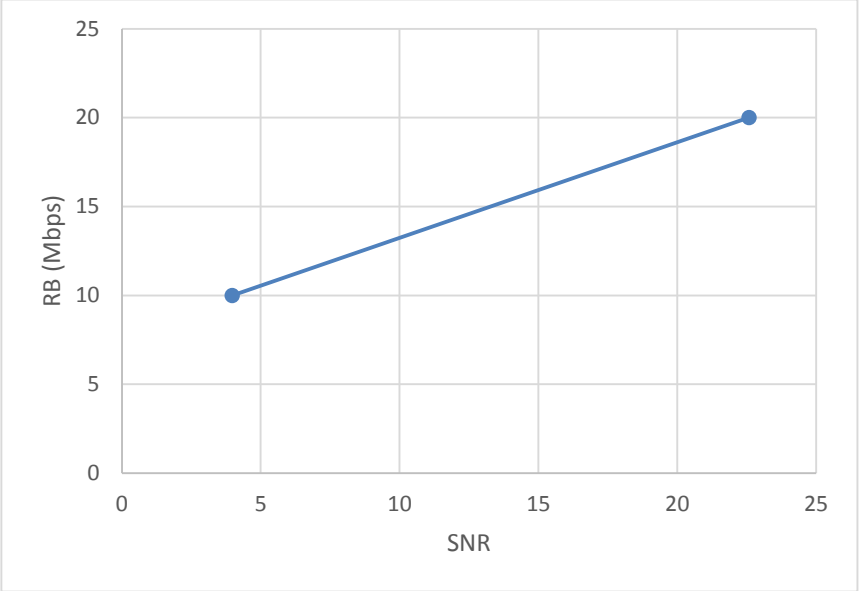
Gráfica. 35. Rb vs SNR QPSK – canal B Tabla 1.

En la gráfica 18 se observa una tasa de transmisión máxima de 20Mbps con un SNR aproximado de 14dB con modulación QPSK con codificación convolucional 1/3.



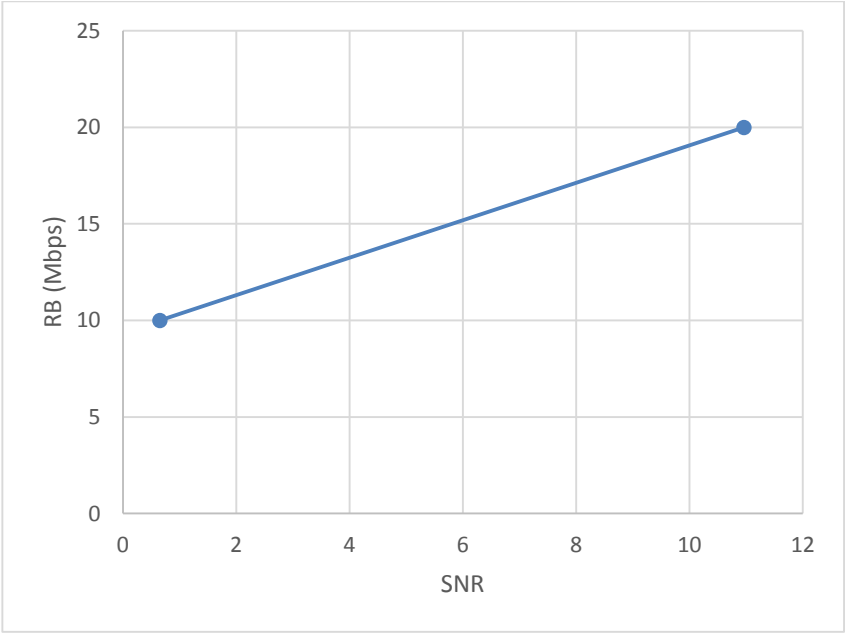
Gráfica. 36. Rb vs SNR PI/4 QPSK – canal AWGN.

En la gráfica 19 se observa una tasa de transmisión máxima de 20Mbps con un SNR aproximado de 21dB con modulación PI/4 QPSK sin codificación.



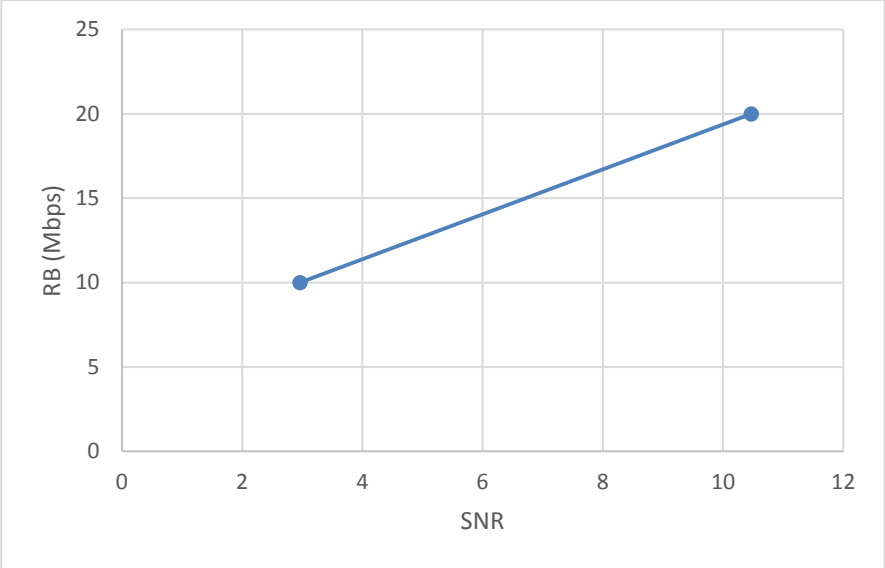
Gráfica. 37. Rb vs SNR PI/4 QPSK – canal AWGN.

En la gráfica 20 se observa una tasa de transmisión máxima de 20Mbps con un SNR aproximado de 23dB con modulación PI/4 QPSK con codificación convolucional 1/3.



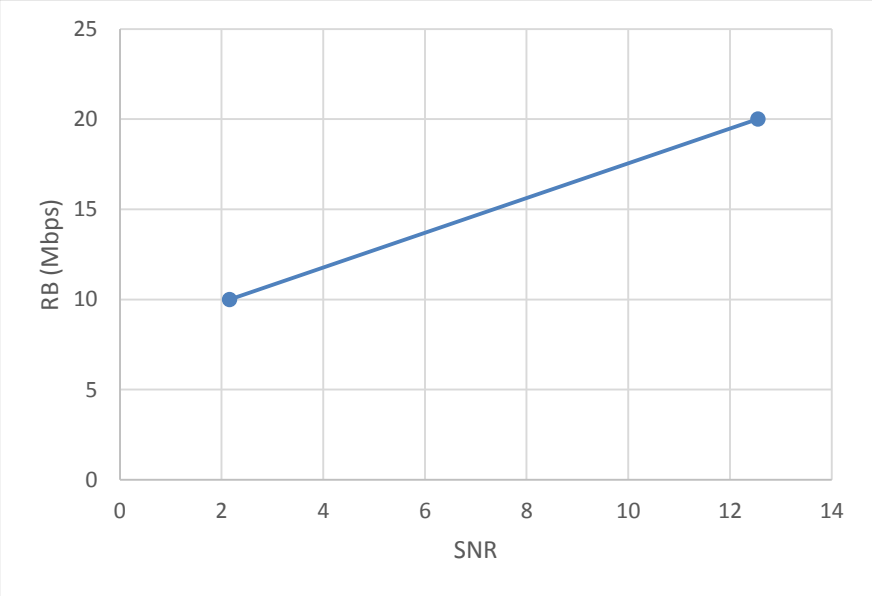
Gráfica. 38. Rb vs SNR PI/4 QPSK – canal A Tabla 1.

En la gráfica 21 se observa una tasa de transmisión máxima de 20Mbps con un SNR aproximado de 11dB con modulación PI/4 QPSK sin codificación.



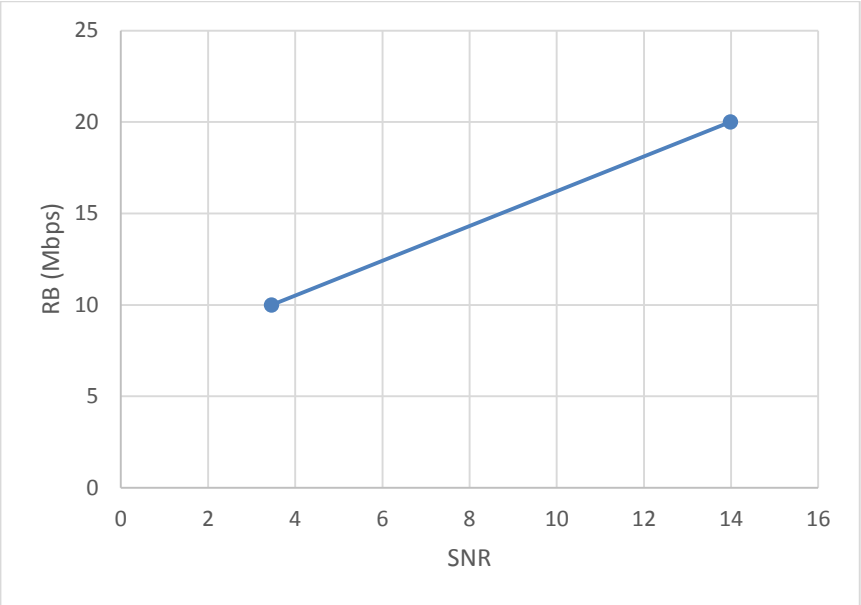
Gráfica. 39. Rb vs SNR PI/4 QPSK – canal A Tabla 1.

En la gráfica 22 se observa una tasa de transmisión máxima de 20Mbps con un SNR aproximado de 11dB con modulación PI/4 QPSK con codificación convolucional 1/3.



Gráfica. 40. Rb vs SNR PI/4 QPSK – canal B Tabla 1.

En la gráfica 23 se observa una tasa de transmisión máxima de 20Mbps con un SNR aproximado de 13dB con modulación PI/4 QPSK sin codificación.



Gráfica. 41. Rb vs SNR QPSK – canal B Tabla 1.

En la gráfica 24 se observa una tasa de transmisión máxima de 20Mbps con un SNR aproximado de 15dB con modulación QPSK con codificación convolucional 1/3.

CONCLUSIONES

Con base en los datos obtenidos con los USRP y con LabVIEW:

- Se observó que tanto QPSK como π/4 QPSK transmiten la misma cantidad de símbolos, son bastantes parecidos, la única diferencia es que π/4 QPSK se encuentra desfasado 45 grados en relación al QPSK normal, por lo tanto esto podría ser de ventaja ya que se pueden usar amplificadores no lineales.

- En un canal con ruido AWGN la señal es más robusta frente al ruido que un canal con ISI con parámetros de áreas rurales, por lo que a potencias de ruido muy altas como -8dB el canal AWGN presenta BER bajo y el mensaje comienza a presentar datos erróneos pero en este punto el mensaje es recuperable, mientras que con un canal de área rural el ruido a potencias de -15 dB comienza a producir un BER bajo en el receptor pero recuperable el mensaje.

- De acuerdo a lo observado en las gráficas de BER vs SNR, el codificador convolucional con tasa de 1/3 realiza una mayor corrección de errores que un sistema con codificación 1/2 y sin codificación.

REFERENCIAS

[1] Gordon L., Stüber, John R. Barry, Steve W. Mclaughlin, Ye(Geoffrey) Li, Mary Ann Ingram, and Thomas G. Pratt, “Broadband MIMO-OFDM Wireless Communication”, Proceedings of the IEEE, Vol.92 ,No.2, February, 2004.

[2] Ebtisam Ahmed, Waqar Aziz, Ghulam Abbas, SaqibSaleem and Qamar-Ul-Islam, “OFDM based Real Time Video Transmision Using USRP”, World Applied Sciences Journal 19 (2): 229-233, 2012, ISSN 1818-4952, IDOSI Publications, 2012 DOI: 10.5829/idosi.wasj.2012.19.02.1269 2012.

[3] Waqar Aziz, Ghulam Abbas, Ebtisam Ahmed, Saqib Saleem and Qamar-ul-Islam, “Design Analysis of Analog Data Reception Using GNU Radio Companion (GRC)”, World Applied Sciences Journal 17 (1): 29-35, ISSN 1818-4952, IDOSI Publications, 2012.

[4] Yong Soo Cho, Jaekwon Kim, Won Young Yang, Chung-Gu Kang, MIMO-OFDM Wireless Communications With MATLAB, Wiley, IEEE Press, 2010.

[5] Fernández Fernández , S. (2004). La Criptografía Clásica. España: SIGMA. Obtenido de http://www.hezkuntza.ejgv.euskadi.eus/r43-573/es/contenidos/informacion/dia6_sigma/es_sigma/adjuntos/sigma_24/9_Criptografia_clasica.pdf.

[6] Pons Martorell, M. (2000). Criptología. Málaga España: Hispasec. Obtenido de http://docplayer.es/8613664-Criptologia-manuel-pons-martorell-escola-universitaria-politecnica-de-mataro-departament-de-telecomunicacions.html.

[7] Sgarro, A. (1990). CODIGOS SECRETOS. Madrid: PIRAMIDE.

[8] Paar, C., & Pelzl, J. (2010). Understanding Cryptography: A Textbook for Students and Practitioners. Berlin: Springer Science & Business Media.

[9] Kumar, Y., Munjal, R., & Sharma, H. (2011). Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures. IJCSMS International Journal of Computer Science and Management Studies, 60-63.

[10] U.S. DEPARTMENT OF COMMERCE National Institute of Standards and Technology. (25 de oct de 1999). DATA ENCRYPTION STANDARD (DES). DATA ENCRYPTION STANDARD (DES). Washington D.C, US: FIPS-Pub.46.

[11] Diffie, W., & Hellman, M. (1977). Exhaustive Cryptanalysis of the NBS Data Encryption Standard. IEEE Computer 10(6), 74-84.

[12] Barker, W., & Barker, E. (jan de 2012). Recommendation forthe Triple Data Encryption Algorithm (TDEA) Block Cipher. Recommendation forthe Triple Data Encryption Algorithm (TDEA) Block Cipher. National Institute of Standards and Technology NIST Special Publication 800-67 Revision 1.

[13] National Institute of Standards and Technology NIST. (26 de nov de 2001). ADVANCED ENCRYPTION STANDARD (AES) . ADVANCED ENCRYPTION STANDARD (AES) . FIPS PUB 197.

[14] Gonzalez, T. (2007). A Reflection Attack on Blowfish. JOURNAL OF LATEX CLASS FILES.

[15] Diffie, W., & Hellman, M. (1976). New Directions in Cryptography. IEEE TRANSACTIONS ON INFORMATION THEORY, 644-654.

[16] Gordon, D. (2001). Designing and Detecting Trapdoors for Discrete Log Cryptosystems. Lecture Notes in Computer Science, 66-75.

[17] Rivest, R., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 120-126.

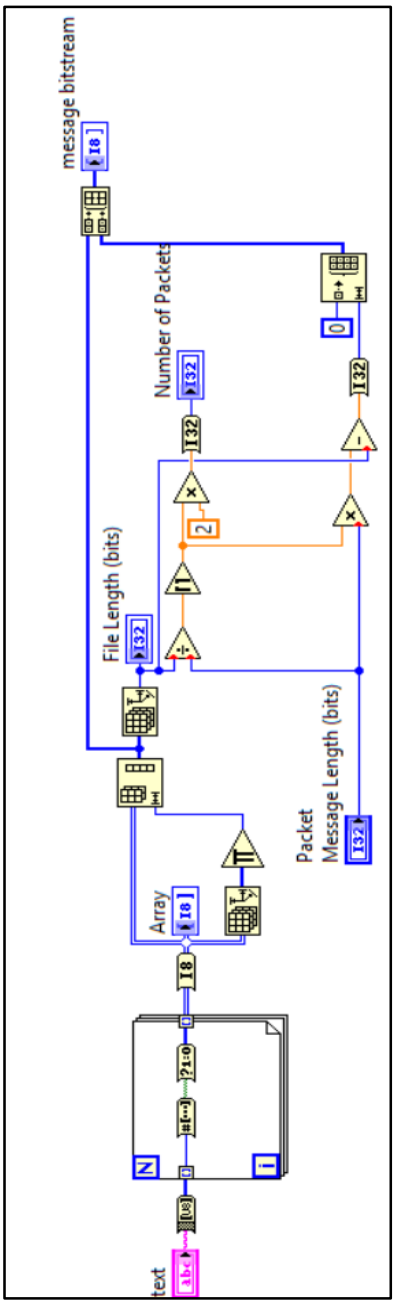
[18] Cormen, T. H., Leiserson, C., Rivest, R. L., & Stein, C. (1990). Introduction to Algorithms. London: MIT Press.

[19] Manual de prácticas del Laboratorio de Comunicaciones Inalámbricas FIEC-ESPOL. Práctica No 4.

ANEXOS

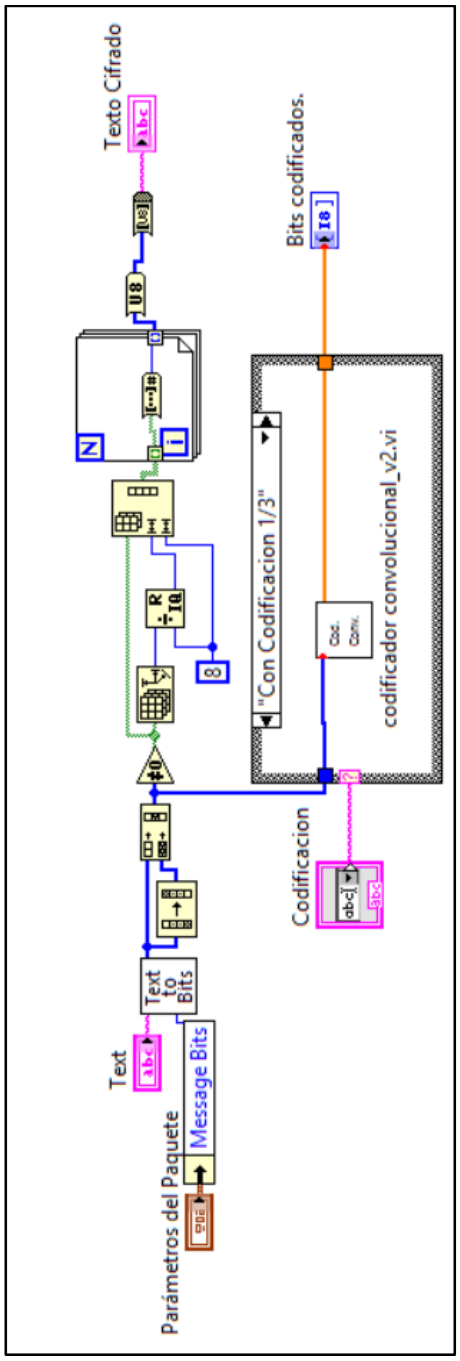
ANEXO 1

DIAGRAMA DE BLOQUE EN LABVIEW DEL CONVERTIDOR TEXTO PLANO EN BITS



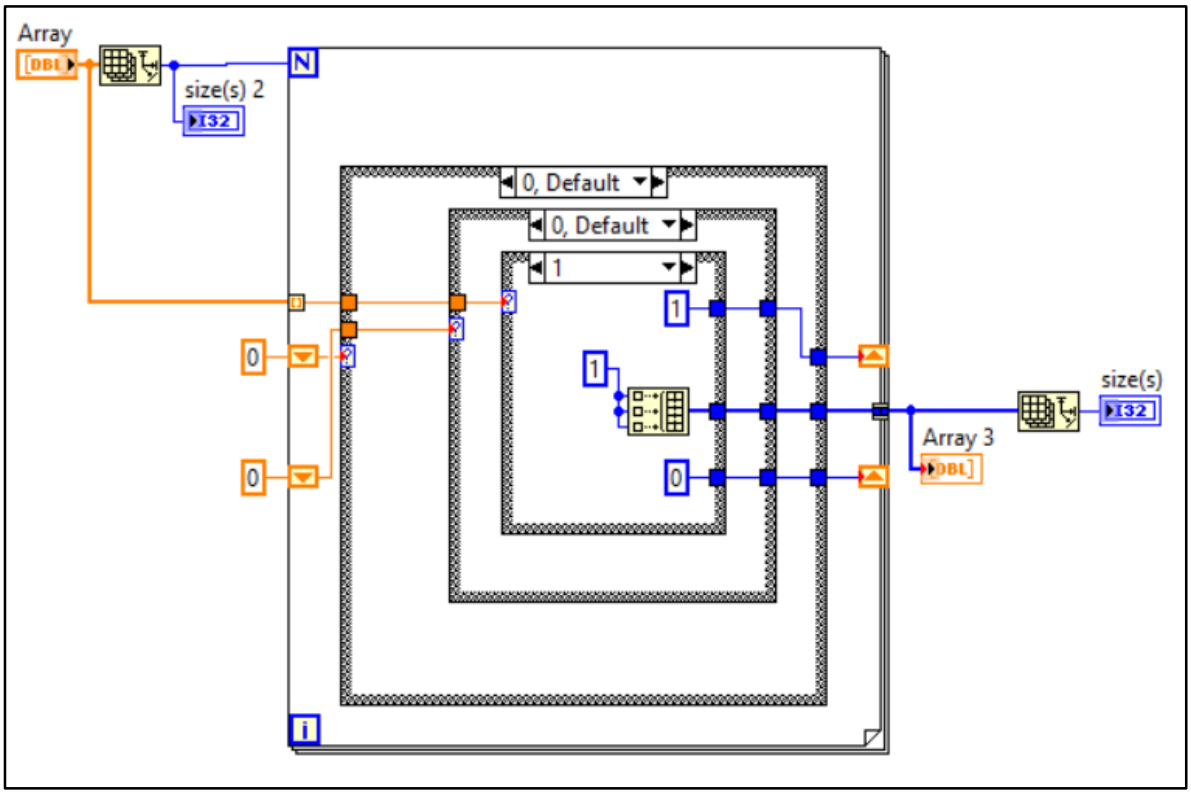
ANEXO 2

DIAGRAMA DE BLOQUE EN LABVIEW DEL CIFRADOR



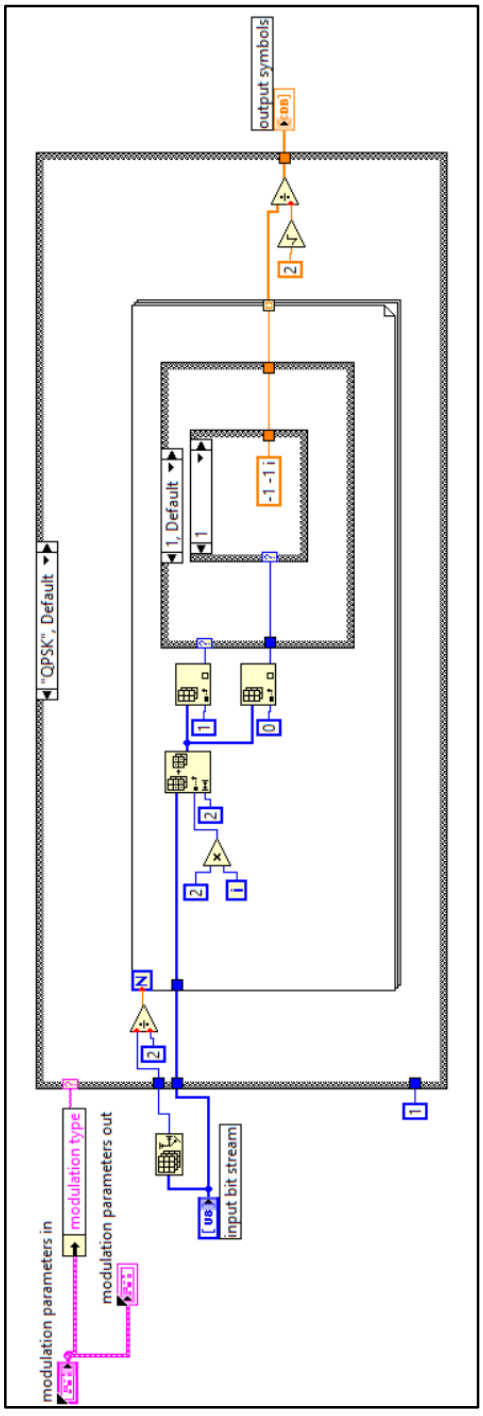
ANEXO 3

DIAGRAMA DE BLOQUE EN LABVIEW CODIFICADOR CONVOLUCIONAL.



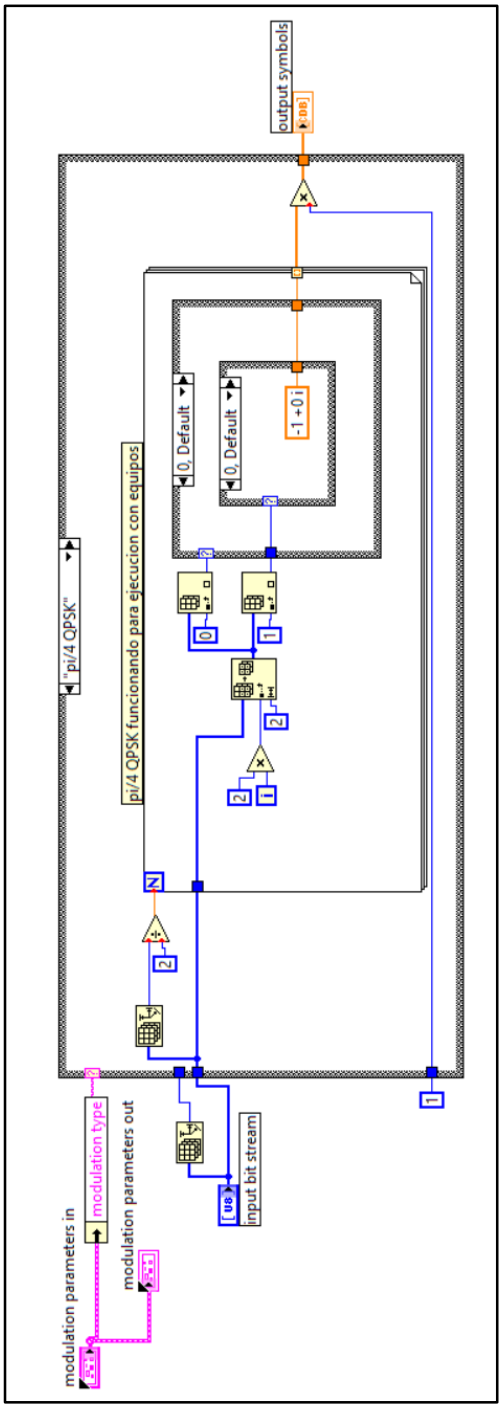
ANEXO 4

DIAGRAMA DE BLOQUE EN LABVIEW MODULACIÓN QPSK.



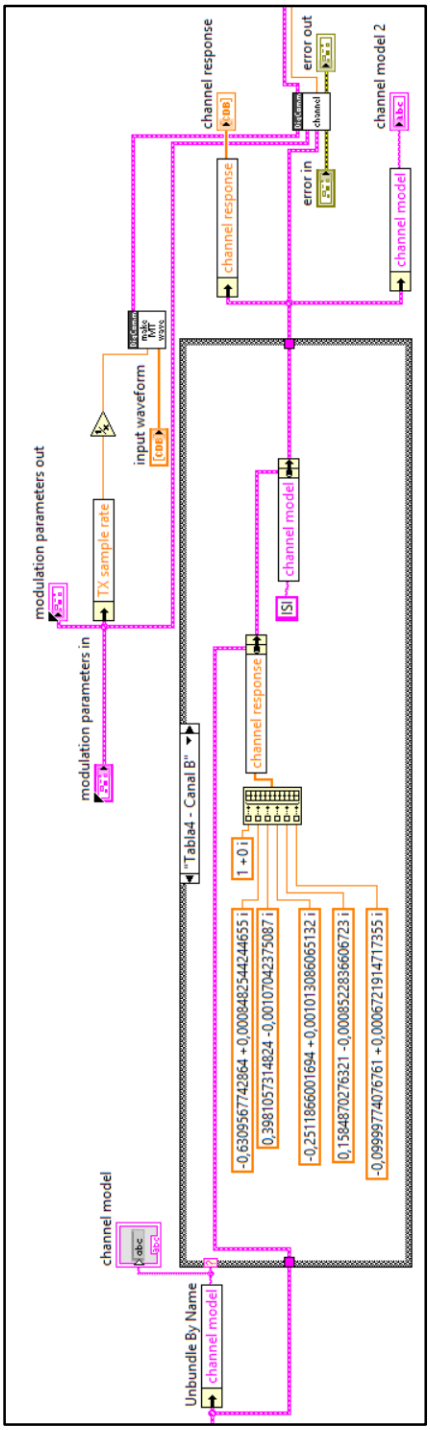
ANEXO 5

DIAGRAMA DE BLOQUE EN LABVIEW MODULACIÓN PI/4 QPSK.



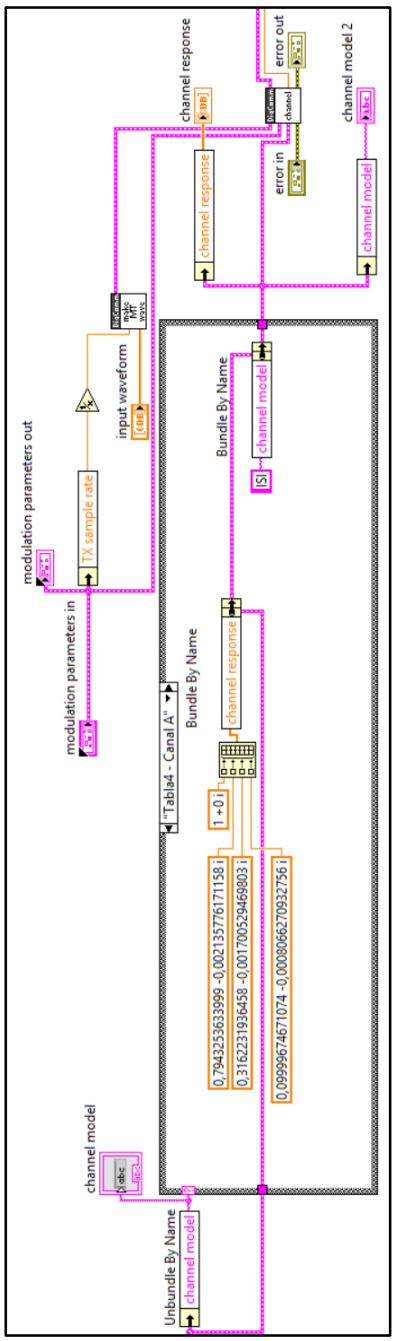
ANEXO 6

DIAGRAMA DE BLOQUE EN LABVIEW CANAL B MULTIPASO – TABLA 1.



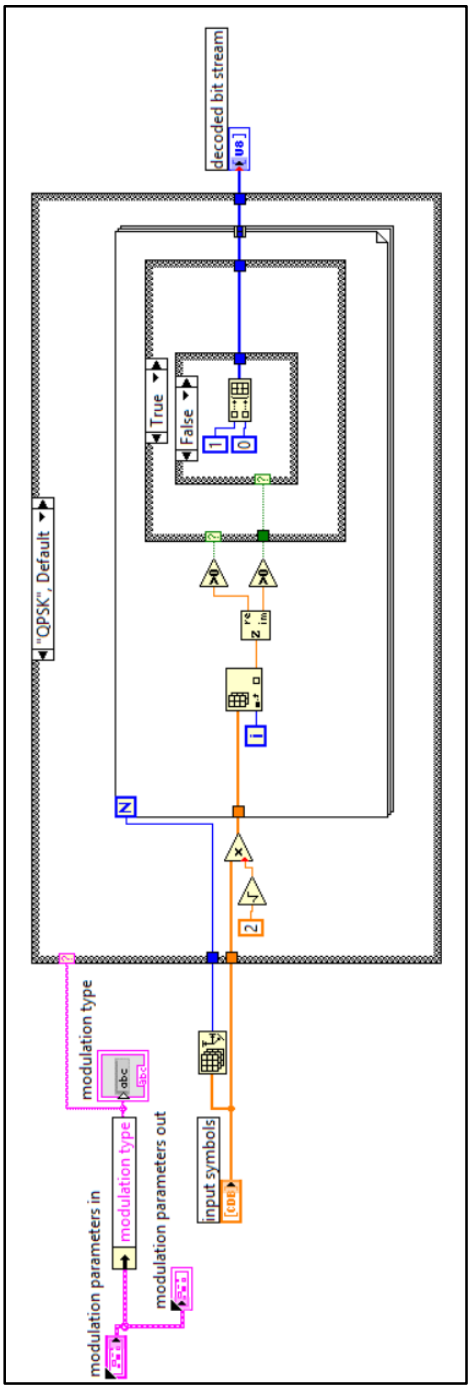
ANEXO 7

DIAGRAMA DE BLOQUE EN LABVIEW CANAL A MULTIPASO – TABLA 1.



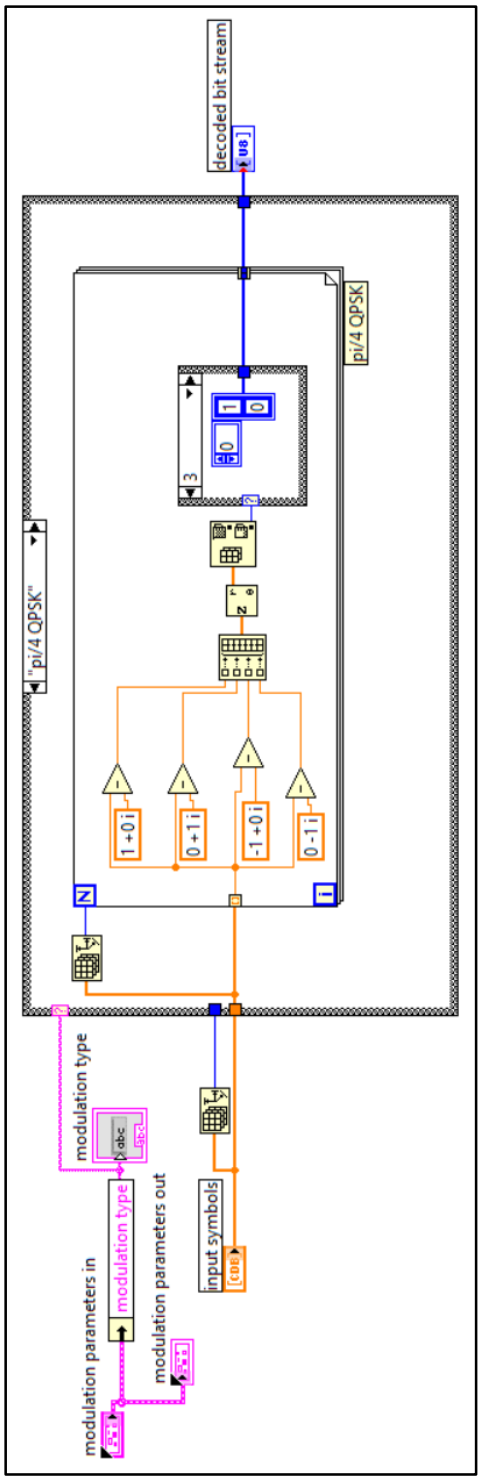
ANEXO 8

DIAGRAMA DE BLOQUE EN LABVIEW DEMODULACIÓN QPSK.



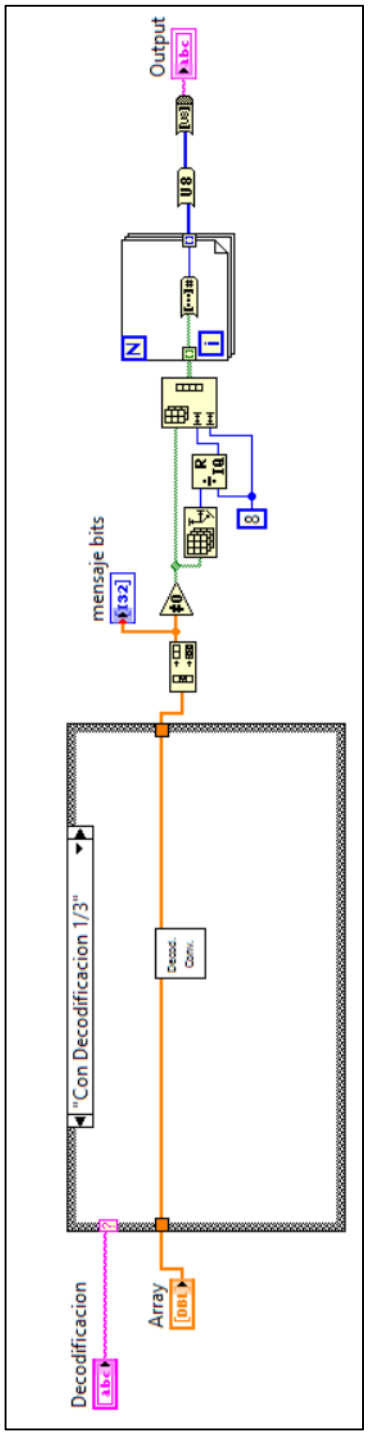
ANEXO 9

DIAGRAMA DE BLOQUE EN LABVIEW DEMODULACIÓN PI/4 QPSK.



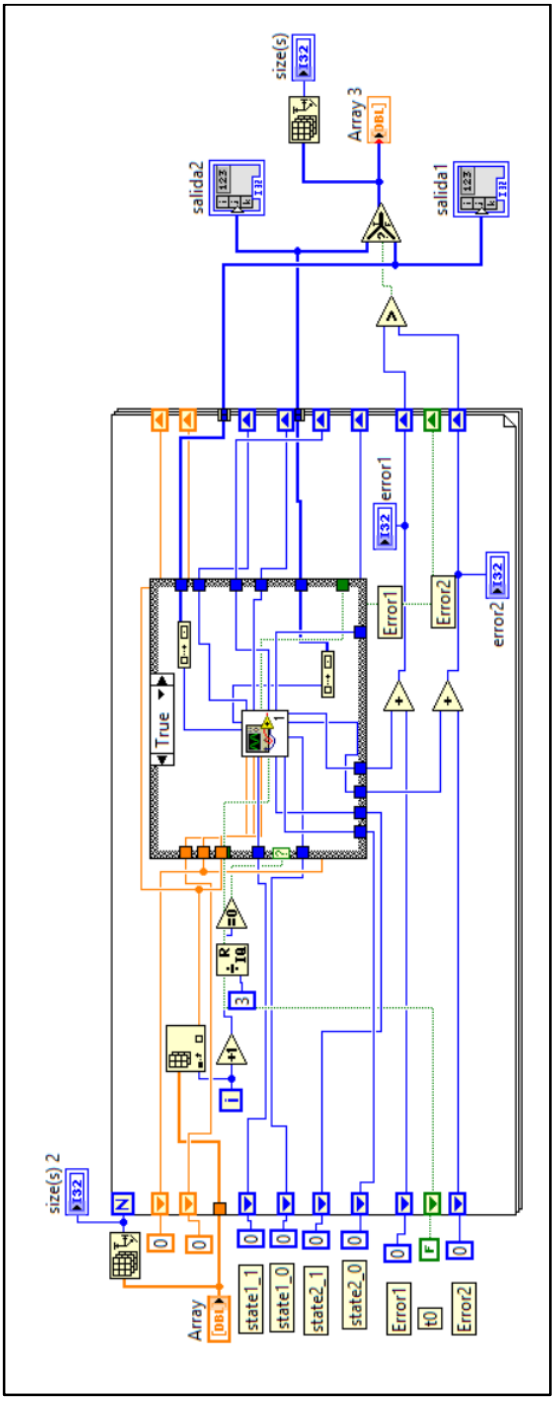
ANEXO 10

DIAGRAMA DE BLOQUE EN LABVIEW DESCIFRADOR Y CONVERTIDOR BITS EN TEXTO PLANO.



ANEXO 11

DIAGRAMA DE BLOQUE EN LABVIEW DECODIFICADOR CONVOLUCIONAL.



ANEXO 12

DIAGRAMA DE BLOQUE EN LABVIEW DECODIFICADOR CONVOLUCIONAL – TRELLIS.